

**UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF TEXAS  
AUSTIN DIVISION**

JASON DAUCH, individually and on behalf of  
all others similarly situated,

Plaintiff,

v.

CLEARRESULT CONSULTING INC.,

Defendant.

Case No. 1:23-cv-01182

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff Jason Dauch (“Plaintiff”) brings this Class Action Petition (“Petition”) against CLEARresult Consulting Inc. (“CLEAR” or “Defendant”), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels’ investigation, and upon information and belief as to all other matters, as follows:

**NATURE OF THE ACTION**

1. Plaintiff brings this class action against CLEAR for its failure to properly secure and safeguard Plaintiff’s and Class Members’ sensitive information, including full names, addresses, phone numbers, emails, Social Security numbers, and solar project and utility account information (“personally identifiable information” or “PII”).

2. Defendant is an energy efficiency consulting company that provides a “variety of integrated technology solutions designed to empower energy providers and organizations” to its clients.<sup>1</sup>

---

<sup>1</sup> <https://www.clearesult.com/products> (last accessed Sep. 25, 2023).

3. Upon information and belief, former and current customers at utility companies that Defendant provides products and/or services to are required to entrust Defendant with sensitive, non-public PII, without which Defendant could not perform its regular business activities, in order to obtain products and/or services from Defendant's clients. Defendant retains this information for at least many years and even after the consumer relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or about May 31, 2023, Defendant learned that one its IT vendor's networks had been penetrated by a cyberattack.<sup>2</sup> In response, Defendant "undertook an investigation with the assistance of external experts to confirm the scope of any potentially affected data."<sup>3</sup> As a result of its investigation, Defendant concluded—on an undisclosed date—that "an unauthorized actor transferred copies of certain files from the CLEAResult MOVEit system on or about May 30, 2023."<sup>4</sup>

6. According to Defendant's Notice of Data Security Incident letter sent to Plaintiff and other victims of the Data Breach (the "Notice Letter"), the compromised PII included individuals' full names, addresses, phone numbers, emails, Social Security numbers, and solar project and utility account information.<sup>5</sup>

7. Defendant failed to adequately protect Plaintiff's and Class Members PII—and

---

<sup>2</sup> The "Notice Letter". A sample copy is available at <https://apps.web.maine.gov/online/aeviewer/ME/40/11a07c54-1d90-4de4-9028-8cc02e794699.shtml> (last accessed Sep. 25, 2023).

<sup>3</sup> *Id.*

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*

failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect consumers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by its IT vendors to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

10. Plaintiff and approximately 12,000 Class Members have suffered injury as a result

of Defendant's conduct.<sup>6</sup> These injuries include: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of their PII; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII.

11. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

### **PARTIES**

12. Plaintiff Jason Dauch is a resident and citizen of Newington, Connecticut. Plaintiff received the Notice of Data Security Incident letter, directly from Defendant, via U.S. mail, dated August 23, 2023 (the "Notice Letter"). If Mr. Dauch had known that Defendant would not adequately protect his PII, he would not have entrusted Defendant with his PII or allowed Defendant to maintain this sensitive PII.

13. Defendant CLEAResult Consulting Inc. is an energy efficiency consulting corporation incorporated under the laws of the State of Texas with its principal place of business

---

<sup>6</sup> According to the breach report submitted to the Office of the Maine Attorney General, 12,723 persons were impacted in the Data Breach. *See* <https://apps.web.maine.gov/online/aevviewer/ME/40/11a07c54-1d90-4de4-9028-8cc02e794699.shtml> (last accessed Sep. 25, 2023).

located at 4301 Westbank Dr., Bldg. A, Suite 250, Austin, Texas 78746-4479, Travis County, Texas. The registered agent for service of process is CT Corporation, 1999 Bryan St., Suite 900, Dallas, Texas 75201-3136.

### **JURISDICTION AND VENUE**

14. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendant.

15. This Court has personal jurisdiction over Defendant because their principal place of business is in the Austin Division of the Western District of Texas and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

16. Venue is proper under 18 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in the Austin Division of the Western District of Texas.

### **FACTUAL ALLEGATIONS**

#### ***Defendant's Business***

17. Defendant is an energy efficiency consulting company that provides a “variety of integrated technology solutions designed to empower energy providers and organizations” to its clients.<sup>7</sup>

18. Plaintiff and Class Members are current and former customers of utility companies that contracted with Defendant for products and/or services.

19. As a condition of receiving products and/or services at Defendant's clients,

---

<sup>7</sup> <https://www.clearesult.com/products> (last accessed Sep. 25, 2023).

CLEAR requires that its clients' customers, including Plaintiff and Class Members, entrust it with highly sensitive personal information.

20. The information held by Defendant in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

21. Upon information and belief, Defendant made promises and representations Plaintiff and Class Members that the PII collected from them as a condition of obtaining energy products and/or services from Defendant's clients would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

22. Indeed, Defendant's Privacy Policy provides that: "[w]e make reasonable efforts to protect your personal information by using physical and electronic safeguards designed to improve the security of the personal information we maintain."<sup>8</sup>

23. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

24. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

25. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify

---

<sup>8</sup> <https://www.clearesult.com/privacy-and-agreement> (last accessed Sep. 25, 2023).

the integrity of its IT vendors and affiliates. Defendant has a legal duty to keep consumer's PII safe and confidential.

26. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

27. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

### ***The Data Breach***

29. On or about August 23, 2023, Defendant began sending Plaintiff and other victims of the Data Breach a Notice of Data Security Incident letter (the "Notice Letter"), informing them that:

**What Happened?** On May 31, 2023, Progress Software Corporation ("Progress") disclosed to all customers, including CLEAResult, that a Progress-owned transfer software tool, MOVEit Transfer, experienced a vulnerability which allowed unauthorized access to the MOVEit Transfer application ("MOVEit Incident"). CLEAResult used MOVEit to transfer files. CLEAResult is one of thousands of organizations worldwide recently affected by the MOVEit Incident.

Upon receiving notice of the MOVEit Incident, CLEAResult immediately took steps to secure its MOVEit application. CLEAResult also undertook an investigation with the assistance of external experts to confirm the scope of any potentially affected data. The investigation revealed that an unauthorized actor transferred copies of certain files from the CLEAResult MOVEit system on or about May 30, 2023. The investigation into the scope of the impact and the information affected is ongoing.

On August 4, 2023, we determined that certain personal data relating to the RRES Program, including your data, was acquired as part of this MOVEit Incident.

**What Information Was Involved?** The impacted information may have included your name, address, phone number, email, Social Security number, and solar project and utility account information.<sup>9</sup>

30. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

31. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

32. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Defendant also stored unencrypted PII on its vendors systems for prolonged periods of time despite warnings against doing so. Moreover, Defendant failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

33. The attacker accessed and acquired files Defendant shared with a third party containing unencrypted PII of Plaintiff and Class Members, including their Social Security numbers and other sensitive information. Plaintiff’s and Class Members’ PII was accessed and stolen in the Data Breach.

---

<sup>9</sup> Notice Letter.



34. Plaintiff further believes his PII and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

***Defendant Acquires, Collects, and Stores Customers' PII***

35. As a condition to obtain products and/or services from Defendant's clients, Plaintiff and Class Members were required to give their sensitive and confidential PII to Defendant.

36. Defendant retains and stores this information and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to perform its services.

37. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

38. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

39. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members or by exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

40. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of

securing PII.

41. Indeed, Defendant's Privacy Policy provides that: "[w]e make reasonable efforts to protect your personal information by using physical and electronic safeguards designed to improve the security of the personal information we maintain."<sup>10</sup>

42. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

***Defendant Knew or Should Have Known of the Risk Because Energy Companies In Possession Of PII Are Particularly Susceptable To Cyber Attacks***

43. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting energy companies that collect and store PII, like Defendant, preceding the date of the breach.

44. Data breaches, including those perpetrated against energy companies that store PII in their systems, have become widespread.

45. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.<sup>11</sup>

46. In light of recent high profile data breaches at industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

---

<sup>10</sup> <https://www.clearesult.com/privacy-and-agreement> (last accessed Sep. 25, 2023).

<sup>11</sup> See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at <https://notified.idtheftcenter.org/s/>), at 6.

47. Defendant knew and understood unprotected or exposed PII in the custody of energy companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

48. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”<sup>12</sup>

49. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

50. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

51. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant’s failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

52. The ramifications of Defendant’s failure to keep secure the PII of Plaintiff and

---

<sup>12</sup> [https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl\\_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=consumerprotection](https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection) (last accessed Oct. 17, 2022).

Class Members, or causing it to be kept secure, are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

53. In the Notice Letter, Defendant offers to cover 24 months of identity monitoring for Plaintiff and Class Members. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members' PII. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

54. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's, or its vendors, computer systems.

55. As a business in custody of its clients' current and former customers' PII, Defendant knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

***Value Of Personally Identifiable Information***

56. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."<sup>13</sup>

---

<sup>13</sup> 17 C.F.R. § 248.201 (2013).

The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”<sup>14</sup>

57. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.<sup>15</sup>

58. For example, Personal Information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>16</sup>

59. Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>17</sup>

60. Social Security numbers, which were compromised for some of the Class Members as alleged herein, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual’s Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply

---

<sup>14</sup> *Id.*

<sup>15</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Oct. 17, 2022).

<sup>16</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Oct. 17, 2022).

<sup>17</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Oct. 21, 2022).

for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>18</sup>

61. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

62. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."<sup>19</sup>

63. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, name, and date of birth.

64. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the

---

<sup>18</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Oct. 17, 2022).

<sup>19</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Oct. 17, 2022).

black market.”<sup>20</sup>

65. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

66. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>21</sup>

***Defendant Fails To Comply With FTC Guidelines***

67. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

68. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

---

<sup>20</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Oct. 17, 2022).

<sup>21</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Oct. 17, 2022).

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.<sup>22</sup>

69. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.<sup>23</sup>

70. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

71. The FTC has brought enforcement actions against energy companies for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. These FTC enforcement actions include actions against energy companies, like Defendant here.

73. Defendant failed to properly implement basic data security practices and/or cause

---

<sup>22</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited Oct. 17, 2022).

<sup>23</sup> *Id.*



its vendors to do so.

74. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

75. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its clients' customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

***Defendant Breached its Duty to Safeguard Plaintiff's and Class Members' PII***

76. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in sharing, obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class Members

77. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect consumers' PII;

- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;
- e. Failing to sufficiently train its employees and vendors regarding the proper handling of its clients' customers' PII;
- f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- g. Failing to adhere to industry standards for cybersecurity as discussed above; and
- h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

78. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

79. Had Defendant remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

### **COMMON INJURIES & DAMAGES**

80. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a)

invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

***The Data Breach Increases Victims' Risk Of Identity Theft***

81. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

82. The unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

83. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

84. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

85. For example, armed with just a name and date of birth, a data thief can utilize a

hacking technique referred to as “social engineering” to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

86. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of “Fullz” packages.<sup>24</sup>

87. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

88. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the

---

<sup>24</sup> “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/) (last visited on May 26, 2023).

PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

89. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

90. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

91. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

***Loss Of Time To Mitigate Risk Of Identity Theft And Fraud***

92. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

93. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant’s Notice Letter instructs,<sup>25</sup> “remain vigilant” and monitor their financial accounts for many years to mitigate the risk of identity theft.

94. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching the Data Breach to obtain more details

---

<sup>25</sup> Notice Letter.

about its occurrence, changing passwords and resecuring their own computer networks, signing up for the credit and identity theft monitoring services offered by Defendant, and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

95. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."<sup>26</sup>

96. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>27</sup>

97. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."<sup>28</sup>

### ***Diminution Value Of PII***

---

<sup>26</sup> See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

<sup>27</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited July 7, 2022).

<sup>28</sup> See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Sep. 13, 2022) ("GAO Report").

98. PII is a valuable property right.<sup>29</sup> Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

99. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other entities in custody of PII often purchase PII on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PII to adjust their insureds' medical insurance premiums.

100. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>30</sup>

101. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.<sup>31,32</sup>

102. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>33</sup>

103. Sensitive PII can sell for as much as \$363 per record according to the Infosec

---

<sup>29</sup> See, e.g., Jason T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at \*3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

<sup>30</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

<sup>31</sup> <https://datacoup.com/>

<sup>32</sup> <https://digi.me/what-is-digime/>

<sup>33</sup> Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html>

Institute.<sup>34</sup>

104. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

105. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., Social Security numbers, date of birth, and names.

106. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

107. The fraudulent activity resulting from the Data Breach may not come to light for years.

108. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

---

<sup>34</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Sep. 13, 2022).



109. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially over twelve thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

110. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

***Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary***

111. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

112. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

113. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.<sup>35</sup> The information

---

<sup>35</sup> See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web*, New Report

disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers).

114. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

115. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant’s Data Breach.

***Loss Of The Benefit Of The Bargain***

116. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant's clients for products and/or services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service that provided the necessary data security to protect their PII, when in fact, CLEAR did not provide the expected data security. Accordingly, Plaintiff and Class Members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant's clients.

**PLAINTIFF DAUCH'S EXPERIENCE**

117. Plaintiff Dauch is a customer of EverSource, which CLEAR provided products and/or services to, and had EverSource install solar panels on his home in or about February 2023.

118. In order to obtain products and/or services at Eversource, he was required to supply Defendant, directly or indirectly, with his PII—including, but not limited to his name, date

---

*Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

of birth, contact information, and Social Security number.

119. Plaintiff Dauch is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

120. At the time of the Data Breach—on or about May 30, 2023—Defendant retained Plaintiff's PII unencrypted PII in a third party system.

121. Plaintiff Dauch received the Notice Letter, by U.S. mail, directly from Defendant, dated August 23, 2023, almost 3 months after the Data Breach, giving the cyber criminals a significant “head start.” According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his full name, address, phone number, email, Social Security number, and solar project and utility account information.

122. Upon receiving the Notice Letter from Defendant, Plaintiff Dauch has spent significant time dealing with the consequences of the Data Breach including researching the Data Breach to obtain more details about its occurrence, changing passwords and resecuring his own computer network, signing up for the credit and identity theft monitoring services offered by Defendant, and checking his financial accounts for any indication of fraudulent activity, which may take years to detect—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

123. Subsequent to the Data Breach, Plaintiff Dauch has suffered numerous, substantial injuries including, but not limited to: (i) lost or diminished value of his PII; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) invasion of privacy; (iv) loss of benefit of the bargain;

and (v) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

124. Plaintiff Dauch further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

125. Plaintiff Dauch also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

126. Plaintiff Dauch has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII being placed in the hands of unauthorized third parties and possibly criminals.

127. Plaintiff Dauch has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

### **CLASS ACTION ALLEGATIONS**

128. Plaintiff brings this action on behalf of himself and all other persons similarly situated.

129. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All persons whose PII was compromised as a result of the Data Breach, for which Defendant provided notice in August 2023 (the "Class").

130. Excluded from the Class are Defendant's officers and directors, and any entity

in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

131. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification.

132. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. At least 12,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Maine's Attorney General's Office.<sup>36</sup> The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

133. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach, or caused its vendors to do so;

---

<sup>36</sup> <https://apps.web.maine.gov/online/aevier/ME/40/11a07c54-1d90-4de4-9028-8cc02e794699.shtml> (last accessed Sep. 25, 2023).

- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their PII;
- f. Whether Defendant breached its duty to Class Members to safeguard their PII;
- g. Whether computer hackers obtained Class Members' PII in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant breached implied contracts for adequate data security with Plaintiff and Class Members;
- l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiff and Class Members;
- m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,
- n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

134. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

135. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

136. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

137. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

138. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

139. Likewise, particular issues are appropriate for certification because such

claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant failed to timely notify the public of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard customers' PII; and
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

140. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

### **CAUSES OF ACTION**

#### **FIRST COUNT**

##### **Negligence**

##### **(On Behalf of Plaintiff and the Class)**

141. Plaintiff re-alleges and incorporates by reference herein all of the allegations



contained in the paragraphs above.

142. Defendant required Plaintiff and Class Members to entrust it with non-public PII in the ordinary course of providing its energy products and/or services.

143. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to its client companies, which solicitations and services affect commerce.

144. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

145. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

146. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach, or cause its vendors to do so.

147. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

148. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure

that its systems and networks, and the personnel responsible for them, adequately protected the PII.

149. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its clients' customers. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of being customers at Defendant's clients.

150. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

151. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

152. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

153. Moreover, Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

154. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard

Class Members' PII;

- b. Failing to adequately monitor the security of their networks and systems;
- c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' PII;
- e. Failing to detect in a timely manner that Class Members' PII had been compromised;
- f. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations,
- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

155. Defendant violated Section 5 of the FTC Act failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

156. Plaintiff and the Class are within the class of persons that the FTC Act intended to protect.

157. The harm that occurred as a result of the Data Breach is the type of harm that the FTC Act intended to guard against.

158. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

159. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

160. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

161. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the energy industry.

162. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

163. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems or on that of its vendors.

164. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

165. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

166. Defendant was in a position to protect against the harm suffered by Plaintiff and

the Class as a result of the Data Breach.

167. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

168. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

169. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

170. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures, and/or causing its vendors to do so.

171. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of their PII; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their PII, which:

(a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII.

172. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to: anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

173. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

174. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

175. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

176. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**SECOND COUNT**  
**Negligence *Per Se***  
**(On Behalf of Plaintiff and the Class)**

177. Plaintiff re-alleges and incorporates by reference herein all of the allegations

contained in the paragraphs above.

178. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant’s duty.

179. Defendant violated Section 5 of the FTC Act and similar state statutes by failing to use reasonable measures to protect PII and not complying with industry standards or causing its vendors to do so. Defendant’s conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant’s systems or that of its vendors.

180. Defendant’s violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

181. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) intended to protect.

182. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

183. But for Defendant’s wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

184. There is a close causal connection between Defendant’s and its vendors failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of

imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

185. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of their PII; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII.

186. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to: anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

187. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

188. Plaintiff and Class Members are entitled to compensatory and consequential



damages suffered as a result of the Data Breach.

189. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

190. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**THIRD COUNT**  
**Breach Of Third-Party Beneficiary Contract**  
**(On Behalf of Plaintiff and the Class)**

191. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the paragraphs above.

192. Upon information and belief, Defendant entered into virtually identical contracts with its clients, including Eversource and other energy companies, to provide products and/or services to them, which included data security practices, procedures, and protocols sufficient to safeguard the PII that was to be entrusted to it.

193. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their PII that Defendant agreed to receive and protect through their products and/or services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties, and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

194. Defendant knew that if they were to breach these contracts with their clients, Plaintiff and the Class, would be harmed.

195. Defendant breached their contracts with its clients and, as a result, Plaintiff and

Class Members were affected by this Data Breach when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

196. As foreseen, Plaintiff and the Class were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the files in their care, including but not limited to, the continuous and substantial risk of harm through the loss of their PII.

197. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

**FOURTH COUNT**  
**Unjust Enrichment**  
**(On Behalf of Plaintiff and the Class)**

198. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the paragraphs above.

199. Plaintiff brings this count in the alternative to the breach of third-party beneficiary contract claim (Count III) above.

200. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for and/or had payments made on their behalf for products and/or services from Defendant and/or its agents and in so doing also provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the products and/or services that were the subject of the transaction and should have had their PII protected with adequate data security.

201. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form their PII as well as payments made on their behalf as a necessary part of their receiving energy products and/or services. Defendant appreciated and accepted that benefit. Defendant

profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

202. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments by, on behalf of, or for the benefit of Plaintiff and Class Members.

203. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

204. Defendant, however, failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

205. Defendant would not be able to carry out an essential function of its regular business without the PII of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

206. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

207. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have allowed their PII to be provided to Defendant.

208. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking

incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

209. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

210. Plaintiff and Class Members have no adequate remedy at law.

211. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of their PII; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII.

212. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

213. Defendant should be compelled to disgorge into a common fund or constructive

trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff prays for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;
- D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
  - i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
  - ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

- iii. Requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- v. Prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

- x. Requiring Defendant to conduct regular database scanning and securing checks;
- xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

- xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and
  - xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
  - xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.
- E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
  - F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;
  - G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
  - H. For an award of punitive damages, as allowable by law;
  - I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
  - J. Pre- and post-judgment interest on any amounts awarded; and
  - K. Such other and further relief as this court may deem just and proper.



**JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury on all claims so triable.

Dated: September 29, 2023

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL

Texas Bar No. 11260700

**KENDALL LAW GROUP, PLLC**

3811 Turtle Creek Blvd., Suite 1450

Dallas, Texas 75219

214-744-3000 / 214-744-3015 (Facsimile)

[jkendall@kendalllawgroup.com](mailto:jkendall@kendalllawgroup.com)

DAVID K. LIETZ\*

**MILBERG COLEMAN BRYSON**

**PHILLIPS GROSSMAN, LLC**

5335 Wisconsin Avenue NW

Washington, D.C. 20015-2052

Telephone: (866) 252-0878

Facsimile: (202) 686-2877

[dlietz@milberg.com](mailto:dlietz@milberg.com)

*ATTORNEYS FOR PLAINTIFF*

*\*PRO HAC VICE FORTHCOMING*